Always use the default scan settings
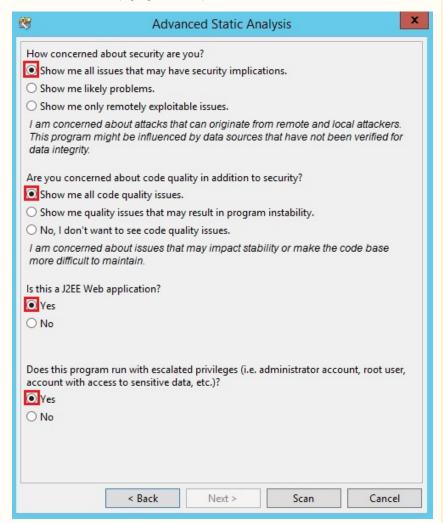
Question

When running a Fortify scan, which settings should I use in answer to the questions "How concerned about security are you," "Are you concerned about code quality," "Is this a J2EE Web application," and "Does this program run with escalated privileges?"

Answer

When running a Fortify scan, it is important to configure everything properly so no issues are hidden or overlooked. When presented with the following screen, you should always use the default values (highlighted in red):

You should always select those options, even if they do not strictly apply to your project. This will ensure the no vulnerabilities or code quality issues will be hidden. As a reminder, no issues should ever be hidden or suppressed.

References

- HPE Fortify Audit Workbench Users Guide - Chapter 2: Scanning Projects

HPE Fortify Version	16.11 and later
Programming Language	☑ C/C++ ☑ .NET ☑ Java ☑ Objective-C ☐ Other
Fortify Audit Workbench	☑ Yes ☐ No
Fortify IDE Plugin	☐ Yes ☐ No
Other Fortify Component	☐ Yes ☐ No

Request code review tools, validations, and support HERE.